

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of:

INFORMATION ASSOCIATED WITH EMAIL
ADDRESS VICTORTIMOTIN@YAHOO.COM THAT
IS STORED AT PREMISES CONTROLLED BY OATH
INC./YAHOO HOLDINGS INC.

)
Case No. 18-M-53
)
)
)
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. §§ 1028, 1028A, 1030, and 1343

The application is based on these facts: See attached affidavit.

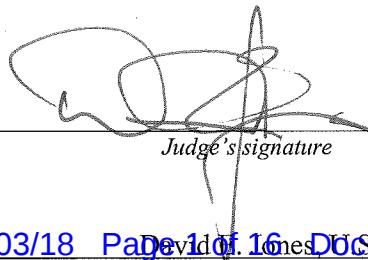
Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

FBI Special Agent Jill Dring
Printed Name and Title

Sworn to before me and signed in my presence:

Date: May 2, 2018


Judge's signature

City and State: Milwaukee, Wisconsin Case No. 18-mj-00053-DEJ Filed 10/03/18 Page 1 of 16 Document 1

Printed Name and Title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jill A. Dring, being duly sworn and under oath state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation. I have been employed with the FBI since May of 2012. I am currently assigned to the FBI Milwaukee Division's White Collar Crimes squad. Between May 2014 and November 2017, I was assigned to the FBI Cyber Crime Task Force.

2. As a Special Agent with the FBI, I have investigated criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of personal identification information, and other computer-based fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received training in computer technology and computer-based fraud.

3. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2713 to require Oath Inc. ("Yahoo") to disclose to the government copies of the information, including the content of communications associated with email address victortimotin@yahoo.com. The account is described in Attachment A. The information to be disclosed by Yahoo is described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. The statements in this affidavit are based on my personal knowledge, information I have received from other law enforcement personnel, publically available information, and

from persons with knowledge of relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation.

5. Based on the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the information associated with the account identified in Attachment A contains evidence and instrumentalities related to violations of Title 18, United States Code, Sections 1030(a)(2)(C) and (a)(5)(A), 1028, and 1028A (the “Subject Offenses”), as described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND OF THE INVESTIGATION

7. Since approximately January 2015, the FBI has been investigating a data breach at a healthcare provider (“HCP”) located in the Eastern District of Wisconsin that involved the use of malware known by the names “Qakbot,” “Qbot,” and “Pinksip Bot” (referred to herein as “Qbot”). During the investigation, the FBI determined that Qbot was being used to record and exfiltrate information, including personal identifying information (“PII”) and financial-related information from compromised computers systems. At this time, Qbot is still being used to access computers without authorization and exfiltrate information from those computers.

6. The Qbot malware is generally considered to be a form of malware known as a “Trojan,” which is delivered to an unsuspecting victim computer system through a corrupted

internet website or in an attachment to an email. The FBI and multiple computer security researchers in the private sector have analyzed the Qbot malware. Based on that analysis, it has been determined that the Qbot malware uses a key logger and form grabber to collect, record, and exfiltrate information from an infected computer system.¹

7. During the course of this investigation, as described below, the FBI determined that the email account freddy100@aol.com was associated with certain domains used by and associated with the Qbot malware. A search of information associated with the freddy100@aol.com account revealed a Webmoney account, which is a digital currency account, was used to pay the cost of registering those domains. Customer records for that particular Webmoney account showed that the Webmoney account was registered using email account victortimotin@yahoo.com.

FACTS IN SUPPORT OF PROBABLE CAUSE

8. In January 2015, the FBI received information from a HCP located in the Eastern District of Wisconsin that it had identified suspicious activity on its computer network. An employee at the HCP determined that the HCP's computer network had been compromised with information-stealing malware. The HCP informed the FBI that it determined that approximately 800 computers operating on its computer network were compromised with the malware.

9. The HCP provided an image of one of the compromised HCP servers to the FBI for analysis. A computer scientist at the FBI analyzed the malware found on the HCP server and determined the malware to be a variant of the Qbot malware. Based on the malware analysis, the FBI determined that the malware damaged each computer it compromised because it modified

¹ A key logger is a type of surveillance software that once installed on a system, can capture any information typed into the computer using the keyboard, including usernames, passwords and other personally identifiable information. A form grabber is a piece of code that works by retrieving authorization and login credentials from a web data form before it is passed over the internet to a secure server, allowing the malware to avoid HTTPS encryption.

existing programs on the compromised computer and installed new programs on the compromised computer.

10. According to the FBI analysis of the Qbot malware, the modified and newly installed programs caused a compromised computer² to execute a series of unauthorized commands that collected and transferred PII, banking information, and other information from the compromised computer to a server identified in the malware. All the information collected through the malware was encrypted and transferred (at the time) to a set of servers located in the U.S. At the time of the FBI analysis, a finite number of IP addresses, which represented servers, were coded into the malware and were utilized to receive the stolen information.

11. On or about August 6, 2015, U.S. Magistrate Judge Nancy Joseph authorized the installation and use of a pen register and trap and trace device or process ("pen-trap device") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to one of the above-described servers receiving stolen data from computers infected with the Qbot malware. Results from the pen-trap device on that server (identified by an IP address) showed communications between the server and IP addresses located³ in multiple foreign countries, including: Australia, Austria, Belgium, Brazil, Bulgaria, Canada, China, Colombia, Egypt, France, Germany, Guyana, Hungary, Indonesia, Israel, Italy, Korea, Lithuania, Mozambique, the Netherlands, New Zealand, Pakistan, Poland, and Russia. Based on my experience and familiarity with this investigation, and information obtained from

² As used in this affidavit, a "compromised" or "infected" computer is a computer on which the Qbot malware has been installed.

³ The terms "IP address" and "server" are used interchangeably in this affidavit. The location of each IP address was determined using Centralops.net, which is a publicly available website that lists contact and registry information for domain names and IP addresses. The information available through that service identifies a service address of the registrant of the IP address. That information was used a substitute for the physical location of server.

other experienced individuals, I believe those communications represented the transfer of stolen information from a compromised computer to the server.

12. The FBI forensic analysis of the Qbot malware revealed that the malware utilizes, among other methods, a domain generating algorithm (“DGA”)⁴ to facilitate communications between a server, referred to as a “command and control server,” and computers infected with the Qbot malware (also known as a “bot”). Based on my training and experience, and information from other experienced agents, I know that a command and control server is used to access and control bots comprising a botnet, or a collection of commonly compromised computers.

13. Based on an analysis of the malware, the FBI determined that on a regular basis, the DGA, which is coded into the malware, generates twenty random domain names⁵ (the “DGA Domains”). The DGA Domains are registered through a domain registration service.⁶ During the registration process, a command and control server, identified by an IP address, is associated with each of the registered DGA Domains.

14. The analysis of the Qbot malware showed that a computer infected with Qbot attempts to connect to a command and control server by calling out the DGA Domains. The infected computer will try each DGA Domain until it successfully connects to one of those

⁴ A DGA is a computer program that creates different variations of domain names based on an algorithm. In this case, the domains names generated by the DGA are comprised of letters from the English alphabet in random order.

⁵ A “domain name” is the unique sequence of alphanumeric characters, separated by periods, that identifies a website on the internet. Unlike an IP address, domain names use letters and words, which are easier to remember. For example, “microsoft.com” is the domain name of Microsoft’s website. When an internet user types that domain name into a computer browser, it directs the computer to connect to the specific web server that contains the specific website files for that domain name.

⁶ Based on my training and experience, I know that in order for a domain to be accessible to over the internet, it must be associated with an IP address. Additionally, companies in the business of registering domains generally require certain information about the registrant of the domain. This information typically includes the registrant’s name and contact information.

domains. Once the infected computer successfully connects to the command and control server through one of the DGA Domains, the person in control of the command and control server can issue commands to the infected computer and control its operation without the owner's authorization.

15. During the course of this investigation, the FBI and multiple private network security firms were able to run the DGA and determine the list of future DGA Domains used by the Qbot malware. Included in that list were the following domains:

zlczwkjpomsmtcawsga.org
qfdjjouamlbqtfyewaxci.org
jdqmdauuzavhvzmchymtn.com
aifrbgvit.org
zwwidimzmcbsrdbrtk.org
uisfhfwqrqcsqcvo.org
gkvimqrvoscnuvggw.net
fobccpaug.org
gjcybzvmvir.com
drufxhimmwwnfhegjbutyw.com
yqwjvhxgaiszygziq.org

16. In March of 2016, BAE Systems utilized the open source tool whois.domaintools.com, to conduct a domain registration analysis for the domains generated by the DGA. At the time that the information was provided to the FBI, the domains listed in the table above were registered with email account fredyu100@aol.com.⁷

17. The FBI analysis of the Qbot malware showed that at the time of the analysis, the malware was configured to use the server associated with IP address 193.111.140.236. Publicly

⁷ BAE Systems is a cyber-security and intelligence firm. BAE provided information related to Qbot to the FBI during the initial stages of this investigation. BAE published a technical analysis of Qbot based on their investigation of the malware. That white paper can be accessed through the following URL: https://media.scmagazine.com/documents/225/bae_qbot_report_56053.pdf

available information shows that the server is located in Germany. U.S. authorities obtained an image of the server associated with IP address 193.111.140.236 using the U.S.-German Mutual Legal Assistance Treaty.

18. A FBI confidential source of information examined a copy of the image of the server associated with IP address 193.111.140.236 and network logs for the server. According to that analysis, the server and log data showed that one of the first commands issued on the server was to connect to the domain youlaamobg.net.

19. In August of 2017, a search of the site whoismind.com⁸ for the email address fredu100@aol.com revealed that domain youlaamobg.net was registered to the email address fredu100@aol.com.

20. On December 12, 2017, U.S. Magistrate Judge David E. Jones Court issued a warrant authorizing the search and seizure of information associated with email account fredu100@aol.com.

21. A review of the information disclosed by Oath Inc./AOL in response to the warrant revealed several emails that were sent to and from the email account that related to the investigation of the Qbot malware. For example, on December 13, 2015, a domain name registration business located in the U.S. sent an email to the account fredu100@aol.com that stated two domains, zlczwkjpomsmtcawsga.org and qfdjjouamlbqtfyewaxci.org, had been successfully registered for a period of 1 year. Specifically, the email stated, “Dear Fedor Antonov, This is a notice that an invoice has been generated on 13/12/15. Your payment method is WebMoney USD.” The email then went on to list the domain names identified in the preceding sentence. As described in paragraph 15, during the FBI investigation of the Qbot

⁸ Whoismind.com is a publically available website that allows users to search for domain registration information.

malware, the FBI identified the domains, zlczwkjposmtcawsga.org and qfdjouamlbqtfyewaxci.org, as DGA Domains.

22. In addition to emails related to the registration of domains used to operate the Qbot malware, I also located an email that listed WebMoney account (Z431310355979) used by “Fedor Antonov.” On November 9, 2015, at 2:44:17 a.m. (EST), the account fredu100@aol.com received an “account activation” email from Goldux.com. In that email, Goldux.com described itself as a “unique e-currency exchange service.” A short time later, at 3:02:51 a.m. (EST), a representative from Goldux.com, using email account admin@goldux.com, sent an email to the account fredu100@aol.com that stated, “Dear client, let us inform you, that your requested amount of 1285.23 USD has been sent to your Webmoney WMZ account Z431310355979.” Based on my training and experience, I know that a Webmoney account that starts with the letter “Z” represents an account based on U.S. currency.

23. On or about March 5, 2018, a Mutual Legal Assistant Treaty request seeking information associated with Webmoney account Z431310355979 was sent from the U.S. to Lithuania.

24. On or about March 12, 2018, the central authority of Lithuania disclosed information associated Webmoney account Z431310355979 to the U.S. According to the information obtained from Lithuania the email account victortimotin@yahoo.com was used to register the Webmoney account. The Webmoney records indicate the email address was “checked,” which I understand to mean that a confirmation email was sent to the account. The financial records associated with the account show significant and frequent transfers in and out of the account. For example, on April 27, 2017, \$60,000 was transferred in to the account. On April 28, 2017, \$61,800 was transferred out of the account.

BACKGROUND CONCERNING EMAIL AND YAHOO

25. In my training and experience, and publically available information from Yahoo, I have learned that Yahoo provides a variety of online services, including email access, to the public. Yahoo members can obtain a free or fee based email account at the domain yahoo.com, like the account victortimotin@yahoo.com, listed in Attachment A. Subscribers obtain an account by registering with Yahoo. During the registration process, Yahoo asks subscribers to provide basic personal information. That information includes the subscriber's name, zip code, date of birth, and in the case of a paid account, billing information, like a credit card number.

26. According to Yahoo's privacy statement, Yahoo also collects the following information from its customers: device information, location information, and usage information.

27. Yahoo states that it uses web beacons, cookies and Software Development Kit (SDK) to collect that information from a user's browser and mobile device. Based on my training and experience, I know that cookies are text files that are placed in a device's browser and can be used to recognize the browser across different browsing sessions. Based on my training and experience, I know that web beacons are small pieces of code placed on web pages, videos, and in emails that can communicate information about your browser and device to a server. Beacons can be used to count users who visit a web page or read an email. They can also be used to deliver a cookie to the browser or the user viewing the web page or email.

28. According to Yahoo, device information relates to the type of device used to access Yahoo services, device identifiers, include IP addresses, cookie information, mobile and advertising identifiers, browser version, operating system type and version, and other information.

29. According to Yahoo, depending on a user's permission settings, Yahoo may collect "pinpoint physical location" information through a user's browser or device. Location information includes the device's GPS signal, Bluetooth connections, nearby WiFi networks, and cell-tower proximity.

30. A more complete description of the vast amount of information Yahoo collects about its customers is located at the following URL:
<https://policies.oath.com/us/en/oath/privacy/index.html>.

31. Based on my training and experience, I believe email in a Yahoo account is stored indefinitely, unless it is deleted. Deleted emails are stored for seven days after they deleted from the account.

32. As described in the preceding paragraphs, the computers of Yahoo are likely to contain stored electronic communications (including retrieved and unretrieved e-mail) and information concerning subscribers and their use of Yahoo services, such as account access information, device information, location information, e-mail transaction information, and account application information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2713 by using the warrant to require Yahoo to disclose to the government copies of the records and other information (including the content of communications), regardless of where they are stored, as described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the information described above, I request that the Court issue the proposed search warrant.
35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Yahoo account victortimotin@yahoo.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Oath Inc./Yahoo Holdings Inc., a company headquartered at 701 First Avenue, Sunnyvale, CA 94089 (the “Provider”).

ATTACHMENT B

Particular Things to be Disclosed and Seized

I. Information to be disclosed by Oath Inc./Yahoo (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on December 22, 2017, the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A since January 2015:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All customer information (e.g. name, age, zip code, date of birth, payment information) associated with the account;
- c. All records and information regarding the creation account and access to the account, including records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, and log-in IP addresses associated with session times and dates;
- d. All records and information and analytics collected by the Provider through the use of browser cookies, web beacons, SDKs, and similar technology;

e. Location information for devices accessing the account, including device's GPS signal, Bluetooth connections, nearby WiFi networks, cell towers, and other types of "pinpoint" location information;

f. Device information including the type of device used to access the account, device identifiers, and the users internet service provider;

g. Log information associated with the account including information about interactions with websites, apps, and other services used by the account holder, the content viewed by the account holder, the search queries submitted by the account holder; and information about how the account holder accesses those websites, apps, and other services, including the browser or operating system of the device, and the website visited before accessing the account;

h. Internet search history;

i. The types of service utilized by the account holder;

j. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

k. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of the warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, and instrumentalities related to violations of Title 18, United States Code, Sections 1030(a)(2)(C) and

(a)(5)(A), 1343, 1028, and 1028A (the “Subject Offenses”), since January 2015, including information pertaining to the following matters:

- a. The identity of the person(s) who created or used the account and devices used to access the account, including records that help reveal the whereabouts of such person(s) such as device information, log information, and pinpoint location information;
- b. Photographs that aid the FBI in identifying the user of the account and the location of the user of the account;
- c. Communications concerning domestic and international travel by the user of the account;
- d. Communications and files stored on the account that relate to Qbot malware;
- e. The identity of the person(s) who communicated with the user of the account including records that help reveal their whereabouts;
- f. Communications to and from the account concerning the use and registration of domains used to facilitate the Subject Offense; and
- g. Communications to and from that account that identify digital currency accounts or other communication facilities used by the user of the account.